

In the United States Patent and Trademark Office

A

Mailed: May 20, 1998

At: Tucson, Arizona

Assistant Commissioner for Patents
Washington, District of Columbia 20231

Sir:

Please file the following enclosed patent application papers:

Applicant #1, Name: John H. Messing
Other Applicant(s): none
Title: Electronic Signature Program

- (x) Specification, Claims, and Abstract: Nr. of Sheets 14
- (x) Declaration: Date Signed: May 20, 1998
- (x) Drawing(s): Number of Sheets Enclosed: (In Triplicate):
 - Formal: 0
 - Informal: 5
- (x) Small Entity Declaration of Inventor(s)
- () Small Entity Declaration of Non-Inventor / Assignee/Licensee
- () Assignment; please record and return; recordal fee enclosed.
- (x) Check for \$ 395.00 for:
 - (x) \$ Filing Fee for filing fee (not more than three independent claims and twenty total claims are presented).
 - () \$ Assignment Fee Additional if Assignment is enclosed for recording.
 - () Return Receipt Postcard Addressed to Applicant #1.
- (x) Request Under MPEP § 707.07(j): The undersigned, a pro-se applicant, respectfully requests that if the Examiner finds patentable subject matter disclosed in this application, but feels that Applicant's present claims are not entirely suitable, the Examiner draft one or more allowable claims for applicant.

Very respectfully,


John H. Messing

Express Mail Label

EE504529905US

; Date of Deposit: 5/20/98

I hereby certify that this document was deposited with the United States Postal Service using "Express Mail Post Office To Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to "Assistant Commissioner for Patents, Washington, DC 20231."

Signed:

Inventor: 

Patent Application of
John H. Messing
for

ELECTRONIC SIGNATURE PROGRAM

Cross References to Related Applications

None.

Background -- Field of Invention

This invention relates to creating and verifying between computers and on computer networks electronic signatures for electronic documents, filings and transaction records.

Background -- Description of Prior Art

An electronic document, legal filing or record of an electronic commercial transaction requires a way to authenticate the parties. Because handwritten signatures on paper have performed the authentication function traditionally, and electronic documents do not allow for this physical method of authentication, electronic substitutes must be found.

Until now, two principally different systems have been devised for "signing" electronic documents, but each has one or more significant drawbacks.

One such system, shown in U.S. Pat. 4,405,829 to Rivest et al. (1983) is based upon a technology known as "asymmetric encryption." In this technology, a user generates two mathematically related numbers that are similar to very long passwords, called keys. The so-called private key remains with the issuing user. The other key, denominated the public key, is distributed by the issuer to others for the purpose of verifying communications. The keys are related, but they are not identical. They perform reverse roles. One is used to encrypt information, and the other to decrypt it.

Electronic communications are signed, generally with the private key, in a two step process. First a digest of a message is created with a one way hash function, and then the hash function is encrypted using the private key. The authenticity of the message and its contents can be verified by a recipient as being authentic and sent from the signing party through testing of the message using the public key. Either an altered message or fraudulent sender will be detected by a computer possessing the proper software, the public key, and the digital certificate of the signer. If the message has been altered or the signer did not use the proper private key, the message will be detected as false. This method is useful for electronic authentication.

However, this method of authentication also requires a massive infrastructure for key management and verification by trusted third parties, called certification authorities, who check the identities of key holders, issue certificates to them verifying that they belong to the party who is identified as the holder of the key pair, and maintain lists of active and revoked certificates for use by relying third parties. Determination of authentication requires not only a check of the digital signature on the message, but also of the status of the certificate identifying the signer, which involves accessing the certificate authority and knowing how to check the lists of revoked and suspended certificates. The investment to create and operate a certification authority is considerable.

Another difficulty with this technology is that private keys are also susceptible to theft from the computers or devices where they are stored, and when stolen, can be used to commit fraud with virtually no detection until the certificate of the user is revoked by the certification authority with respect to that particular corresponding public and private key pair.

The creation and maintenance of the certification authority infrastructure requires a massive investment in equipment and personnel that results in a relatively high cost to the end user where suitable means are adopted by the certification authority to verify the true identity of a holder of a private key before issuance of a digital certificate to the alleged owner of the key.

Furthermore, in business and legal settings where both parties are required to electronically sign documents, filings or transaction records using their respective private keys and digital certificates, and they are located in or claim citizenship of different legal jurisdictions or countries, there is a possibility for uncertainty or actual conflict in the laws applicable to the transaction. In some countries, users may be required to give copies of the keys to the applicable governmental authority upon pain of punishment. This requirement may compromise the privacy and security of the electronic signatures. Where different legal regimes are involved, such uncertainty or conflict may actually impede the use of the electronic signatures for fear by participants of legal attacks from overzealous authorities or corrupt ones, depending on the reputations of the countries involved and their political regimes.

PenOp, U.S. Pat. No. 5,554,255(1994), and continuation serial number 298,991, U.S. Patent 5,647,017 (1997) and related patents cited therein, adopts a completely different approach to electronic signatures. It uses digital drawing tablets as a basis for digitally capturing a handwritten signature, and then through software stores certain signature characteristics which identify the dynamic movements of the writer's hand as it moves the stylus on the tablet during signature creation, in addition to the image of the signature on the tablet. This stored information is then compared to a subsequently generated signature

to determine if the signature is authentic. If a hash function is captured, digested, and linked to the document, this approach, like the "digital signature" approach of the "asymmetric encryption" can determine any changes that have been made to the document since the signature was applied.

This "dynamic signature" approach avoids the massive infrastructure of the "public key encryption" certification authorities, and the problem of conflicting legal regimes applicable to electronic signing of documents in an international or multi-jurisdictional setting, but it requires the provision of a digital drawing tablet and stylus at each computer workstation where signature is to be accomplished, as well as the related software, which can be a significant system-wide item of cost. In addition, traditional forensic analysis applicable to handwritten signatures does not yet apply to electronic signature analysis, and it may be some time, if ever, before the legal forensic community becomes adept at dynamic signature handwriting analysis. Because there is no way at present for expert analysis of dynamic signatures, the ability to authenticate signatures is arguable at best.

In addition, these technologies are mutually exclusive, in that one cannot incorporate the other, and it is not possible to use them together under prior art.

Objects and Advantages

Accordingly, several objects and advantages of the invention are to provide a new type of electronic signature that does not depend upon the massive certification authority infrastructure of digital signatures based on asymmetric encryption or the hardware and software investment of dynamic signatures; further that it uses only one signature key of the server computer located in and subject to the jurisdiction only of the political authority of the server computer, further that it automatically generates and affixes a date and time stamp as proof of those parameters at the time of the signature; further that it eliminates the need for development of a discipline that does not yet exist, namely, the forensic science of electronic handwriting analysis; and that further allows for the use by incorporation of the

other two forms of authentication into its system, as well as others that exist or may emerge in the future.

Still further objects and advantages will become apparent from a consideration of the ensuing description and accompanying drawings.

Drawing Figures

Fig. 1 shows authentication as a means of access by a web browser to a web server.

Fig. 2 shows how a web server "parses" or separates out for storage certain information transmitted by a web form page.

Fig. 3 shows the creation of the signature from database submission information and the system clock.

Fig. 4 is a representation of the machine process whereby the computer takes the signature token, wraps it in a digital wrapper, and signs it with the server's private key.

Fig. 5 is a representation of a web page as shown to the user which contains the signature button for signing the document.

Summary

In accordance with the present invention, an electronic signature program is described for the creation, monitoring, and verification of an electronic signature generated by the interaction between two computers for the signing of documents, filings or transaction records without the need for an expensive and massive infrastructure of certification authorities, without generating conflicts between applicable legal regimes in an international or multi-jurisdictional setting over regulation of encryption software, or without requiring hardware tablets and associated computer software. This system further

is able to incorporate other existing technologies designed to authenticate users and ones not yet available or existing.

Description – Figs. 1 to 5

The electronic signature is affixed between computers over the Internet. Figure 1 depicts the initial contact between an Internet user and an Internet server. This is accomplished by ordinary web browser. A method for authenticating users allows the additional option to screen out unauthorized users (fig. 1, no. 12). To access the signature device, users must pass the authentication gateway. Where unauthorized users are to excluded, many different systems of screening out unauthorized computer users can be utilized, including but not limited to digital certificates to users from trusted third parties, previously issued passwords, stored and verifiable dynamic signatures, credit card authorizations, retinal scans and other authentication methods, without limitation. Unless the system is open to all users, unauthorized users are rejected by the system using the authentication system. If the system is open, the authentication mode is universal, and all users are permitted to create electronic signatures.

Information is collected from the users as shown in figure 2, (no. 14). It is transmitted for the purpose of (no. 15), parsing (separating out discrete information supplied by the user upon submission of a web page form that is specific to a filing, document or transaction)(no. 16) and storage of the information on the server computer (no. 17).

Creation of the signature is depicted in figure 3. Certain information from the user elements (no. 18) are combined with the date-time stamp of the system clock (no. 19) to create a unique blend of the components. (no. 20). This combination also permits a date and time stamp to be incorporated into the signature.

Figure 4 demonstrates how the signature is encapsulated in the digital signature of the server computer. An active X (com) object or other applications programming interface

(API)(no. 23) at the Internet server creates a digital wrapper (no. 24) and communicates with the signature program of the Internet server to sign the information (no. 22) contained in the signature (no. 21) with the server's private key. Once the signature is thus encapsulated and digitally signed, it is included in an automatically generated email message (no. 25). It is sent to the user at the email address that the user self-reported to the Internet server initially.

The digitally signed wrapper ensures that the information included in it, including transaction particulars, date and time stamp, and electronic signature cannot be altered after the fact without such change being detectable through software. Return of this information to the individual who signed the information is a receipt that is proof of the transaction, the electronic signature, and the transaction content.

If the email address is non-existent, intermediate mail server computers usually alert the server via a failed email message that the message was undeliverable. Such a message also serves to warn the server computer that a fraudulent transaction may be in progress.

Figure 5 depicts the mechanism for actually invoking the signature device, as viewed by the user. A simple button (no. 23) is clicked by the user, coupled with a clear warning (no. 24) of the consequences of clicking the signature button. Once the button is clicked, the electronic signature feature is enabled.

If the email receipt containing the electronic signature is received by the signer, that individual optionally may be required to countersign the receipt digitally (preferably using asymmetric encryption) and then to return the resigned message back to the server computer for storage and as further proof of receipt and authentication. This receipt at the server computer proves that the user actually received the electronically signed message, and the digital signature can be stored at the server as a further guarantee of message authenticity.

Conclusions, Ramifications, and Scope

Accordingly, it can be seen that the above system allows computer users to sign electronic documents, filings and transaction records submitted to another computer as though with pen and ink on paper, without any additional hardware or software apart from an Internet web browser. The signature program reduces the need for a massive infrastructure investment of certification authorities by relying solely upon the digital certificate of the server computer, without any similar requirement that the signing party obtain a separate digital certificate, unless optionally required for receipt signing purposes. The program eliminates certain legal problems that may arise from attempts by multiple legal regimes to regulate encryption features of asymmetric encryption program, through key recovery programs, since only one key, that of the server computer is involved, and only one legal regime will likely be entitled to regulate the server. The program is able to make use of other current and future technologies for computer user authentication systems, and is suited for the Internet and other computer networks.

Although the description above contains much specificity, this should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. Various other embodiments and ramifications are possible within its scope. For example, and not by way of limitation other unique system information of the server can be used in addition to or instead of the system clock to generate a unique signature token. Similar, the signature and the filing, document or transaction record to be signed and be digitally wrapped and signed using techniques other than asymmetric encryption.

Thus the scope of the invention should be determined by the appended claims and their legal equivalents, rather than by the examples given.

Claims: What is claimed is:

Electronic signature patent:

I claim:

1. An electronic signature program for the creation, monitoring, and verification of an electronic signature, comprising:
 - (a) an authentication device or method,
 - (b) a central processing unit with a memory, said central processing unit being connected to receive data from said authentication device or method, either directly by accessing physical storage or over a computer network, including but not limited to the Internet, and to provide verification of the right of a user of another computer to access the computer of said central processing unit;
 - (c) a device or method for requesting and collecting unique data from an authenticated user for the purpose of receiving, creating, or assembling an electronic document, filing and/or transaction record;
 - (d) a parser to separate out information supplied by the authenticated user as unique to the document or transaction being signed as opposed to routinely supplied template or boilerplate related to such transaction, said parser being operated by said central processing unit;
 - (e) a first storage unit for collecting and archiving said unique information of the authenticated user, said first storage unit being connected to said central processing unit of said receiver computer,

- (f) a second resolving unit for combining said unique information of the authenticated user with quantitative parameters of the receiver computer, said second resolving unit being connected to said central processing unit and said first storage unit;
- (g) a method or device for digitally wrapping said unique information of the authenticated user together with the unique information of the server computer in combination with or apart from the said electronic document, filing or transaction record;
- (h) a method or device for creating digitally signed messages with a plurality of data parameters, said digital signature being capable of authentication pursuant to asymmetric encryption or other digital signature verification method, without limitation, being connected to said central processing unit and said first storage unit; and/or said second resolving unit;
- (i) a dispatching unit or method for returning the digitally signed, wrapped document, transaction information, other unique information, together with the electronic signature over the Internet or other computer network to the computer from whence it originated as proof of receipt of the unique information and the related electronic signature used to sign the contents thereof;

2.The electronic signature program of claim 1 wherein a method or unit is used for creating an archival copy at the receiver computer of the document, filing, transaction, and any other particulars of the process and interchange of information, and the electronic signature of the same on a medium which is not susceptible to change or modification thereafter.

3.The electronic signature program of claim 1 wherein the unique system information of the server computer consists of the date and time as reported from time to time to the memory locations of the central processing unit.

4. The electronic signature program of claim 1 wherein a digitally signed reply is further required of the signer as an additional receipt and authentication procedure.
5. The method of claim 1 wherein a unit is used for storing data in appropriate form for archival purposes, said archival unit being connected to said second resolving unit and having write-once, read-only properties.
6. The electronic signature program of claim 1 wherein the computer data containing the electronic signature is digitally signed at the server computer by a method other than asymmetric encryption.
7. The electronic signature program of claim 1 wherein said electronic signature is used for legal documents that are thereafter transmitted to and filed electronically with courts, regulatory agencies or document repositories as original legal filings.
8. The electronic signature program of claim 1 wherein the integrity of the electronic signature and the document it signed is verified through use of the corresponding public key of the receiver computer.
9. An electronic signature program for generating and returning an electronic signature between two computers whereby a receiving computer
 - (a) obtains a plurality of parametric data from a user of another computer over the Internet, other computer network, or pursuant to physical storage medium;
 - (b) converts each datum obtained into storage units parsed by the receiving computer from the value of each datum within the information datum provided by the user;
 - (c) combines such information datum with unique data of the receiving computer generated for each such transaction with a user;
 - (d) affixes a digital signature to the resultant information datum; and

(e) returns the digitally signed information datum to the user.

10. The electronic signature program of claim 9 wherein said related parameters are user supplied data of a signer and said data is combined with unique information of the recipient computer and allows authentication of user and message contents by means the electronic signature of such user as verified by the unique identifier of the server computer and differential deviations with those for a known unauthorized signature or modified message content.
11. The electronic signature program of claim 9 wherein a method or unit is used for creating an archival copy at the receiver computer of the document, filing, transaction, and any other particulars of the process and interchange of information, and the electronic signature of the same on a medium which is not susceptible to change or modification thereafter.
12. The electronic signature program of claim 9 wherein a digitally signed reply is required of the signer as a further receipt and authentication procedure.
13. The electronic signature program of claim 9 wherein a unit is used for storing data in appropriate form for archival purposes, said archival unit having write-once, read-only properties.
14. The electronic signature program of claim 9 wherein the signature is affixed by pressing a button on a form presented by the receiver computer.
15. The electronic signature program of claim 9 wherein the information requested of the user is provided by a form presented by the server computer to the computer of the signing party.

16. An electronic signature program to create a legally binding signature for electronic documents, filings and transactions over the Internet, and other computer networks, comprising the steps of:

- (a) authenticating the user by one of several means;
- (b) obtaining unique information related to the document or transaction to be effectuated by means of forms completed by the user;
- (c) providing a means to incorporate certain such user supplied information relating to the transaction with the system clock information of the server computer;
- (d) digitally signing the combined user supplied information and server clock information; and
- (e) transmitting the signed information back to the user as a receipt containing the document or document information and the electronic signature of the computer user.

17. The electronic signature program of claim 16 wherein the information requested of the user is provided by a form presented by the server computer.

18. The electronic signature program of claim 16 wherein a unit is used for storing data in appropriate form for archival purposes, said archival unit having write-once, read-only properties.

19. The electronic signature program of claim 16 wherein a digitally signed reply is required of the signer as a further receipt and authentication procedure.

ELECTRONIC SIGNATURE PROGRAM

Abstract:

An electronic signature program to create an electronic signature for documents, filings, and transactions records effectuated between computers. A computer user is authenticated by a server computer. The computer user supplies certain information to the server computer, which extracts the information, and when a signature command is received, combines certain of the user submitted information with certain predetermined elements of the system information of the server, then digitally signs this combination of information along with the document, filing or transaction record which is being signed. The digitally signed combined information is returned to the user as the user's electronic signature of the information which was submitted for signature, together with the signed information, being the document, filing, or transaction record itself.

2025 RELEASE UNDER E.O. 14176

In the United States Patent and Trademark Office

First/Sole Applicant: John H. Messing
Other Applicant(s): None
Title: "Electronic Signature Program"

Small Entity Declaration - Independent Inventor(s)

As a below-named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35 United States Code, to the Patent and Trademark Office with regard to my above-identified invention described in the specification filed herewith. I have not assigned, granted, conveyed, or licensed and am under no obligation under any contract or law to assign, grant, convey, or license any rights in the invention to either (a) any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or (b) any concern which would not qualify as either (i) a small business concern under 37 CFR 1.9(d) or (ii) a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

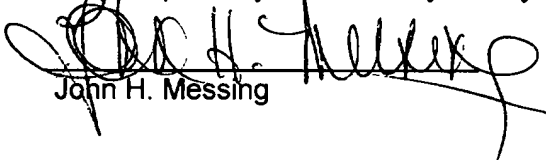
- (x) There is no such person, concern, or organization.
() Any applicable person, concern, or organization is listed below:

Full Name: None
Address: None

I acknowledge a duty to file, in the above application for patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Very respectfully this 20th day of May 1998,


John H. Messing

Declaration for Utility or Design Patent Application

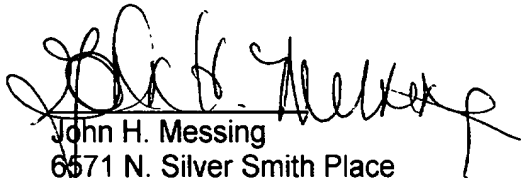
As a below-named inventor, I hereby declare that my residence, post office address, and citizenship are as stated below next to my name and that I believe that I am the original, first, and sole inventor [if only one name is listed below] or an original, first, and joint inventor [if plural names are listed below] of the subject matter which is claimed and for which a patent is sought on the invention, the specification of which is attached hereto and which has the following title:

"Electronic signature program"

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration. I acknowledge a duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, Section 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Please send correspondence and make telephone calls to the First Inventor below



John H. Messing
6671 N. Silver Smith Place
Tucson, AZ 85712
U.S. Citizen
Tel.: (520) 327-7750
Or (520) 529-3275
Fax: (520) 327-7722
Email: jmessing@law-on-line.com

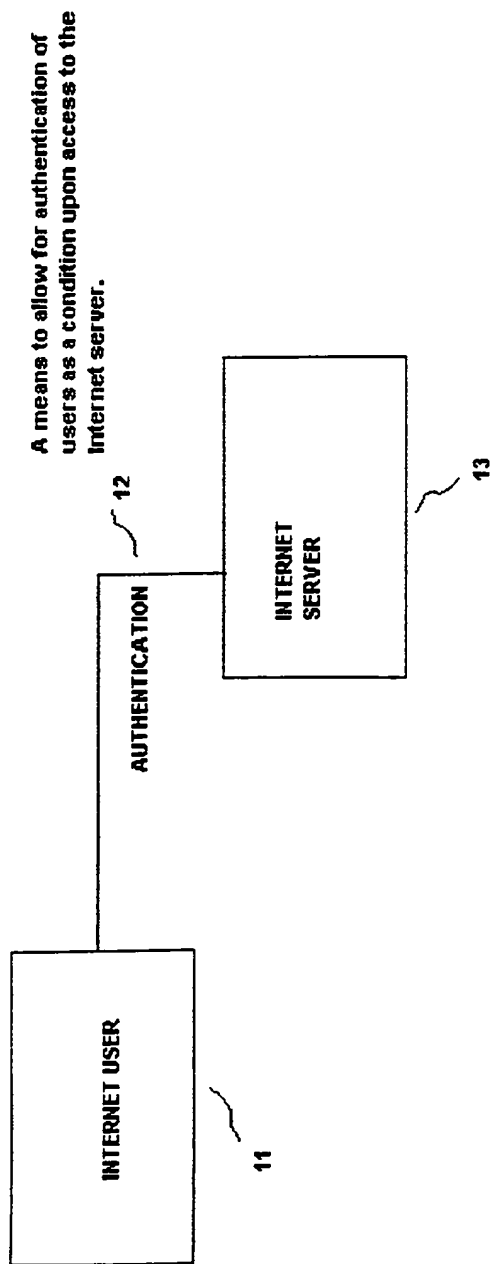


Figure 1

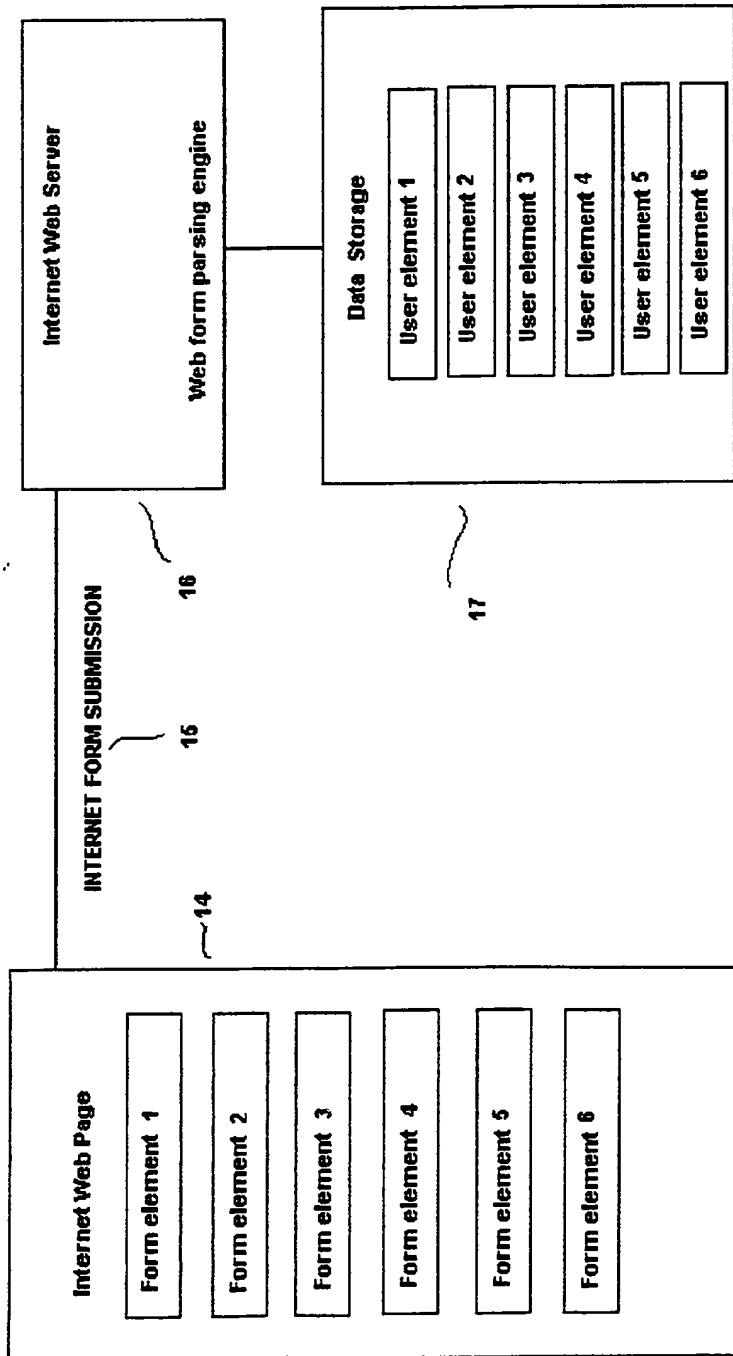


Figure 2

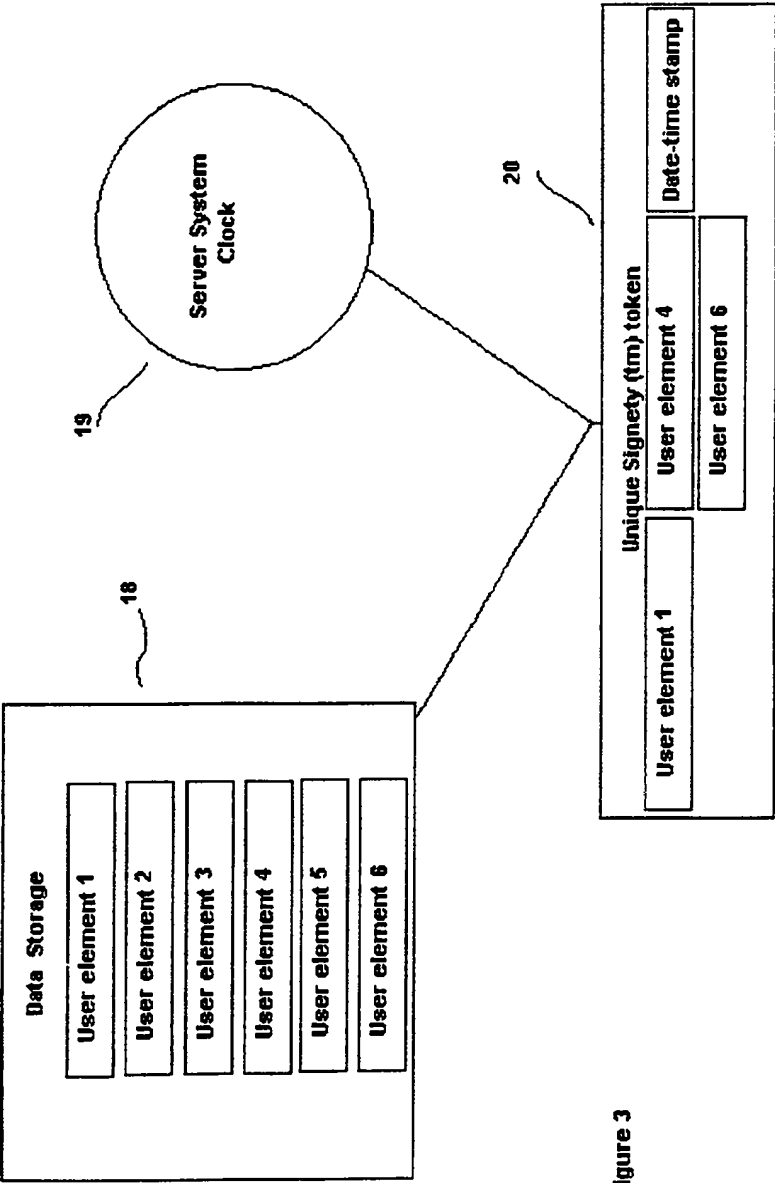


Figure 3

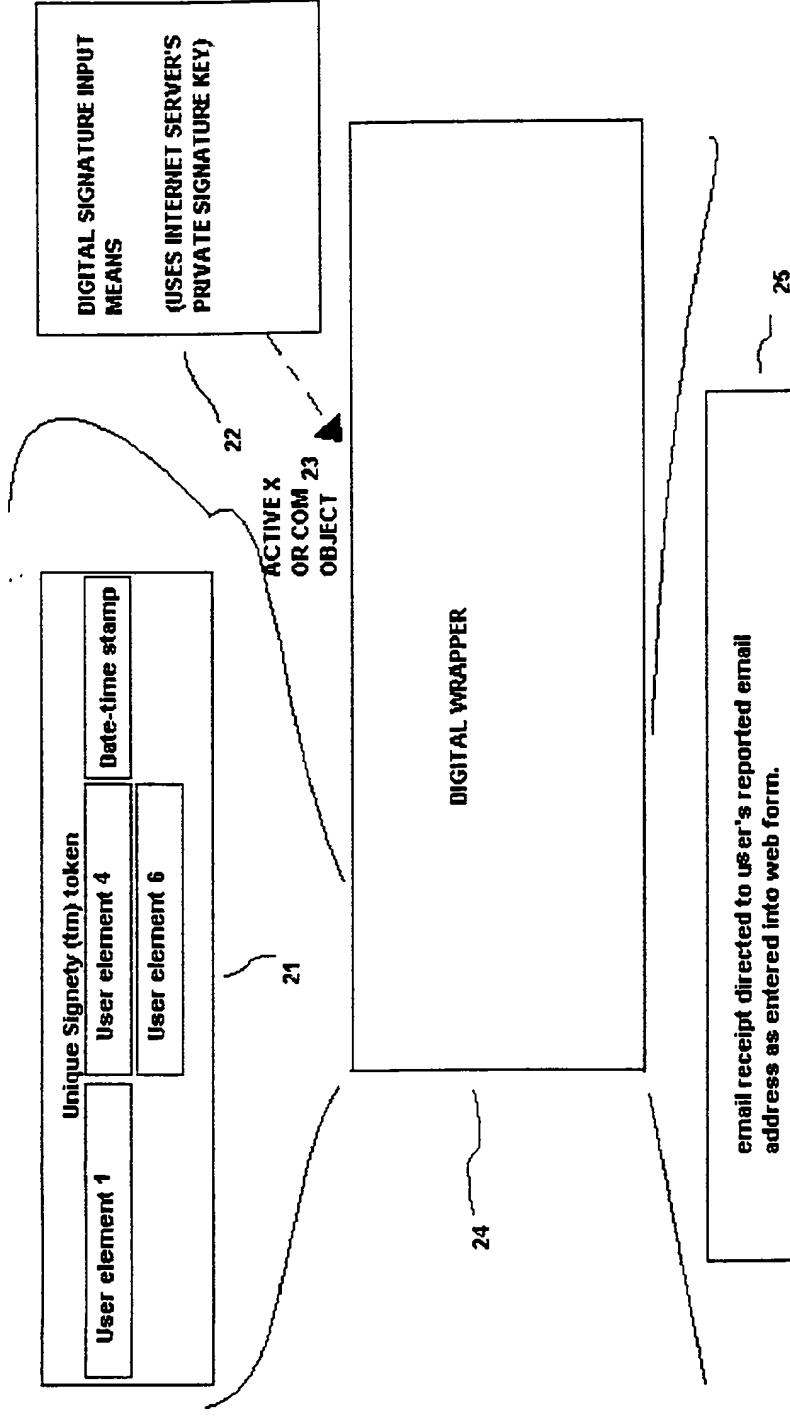


Figure 4

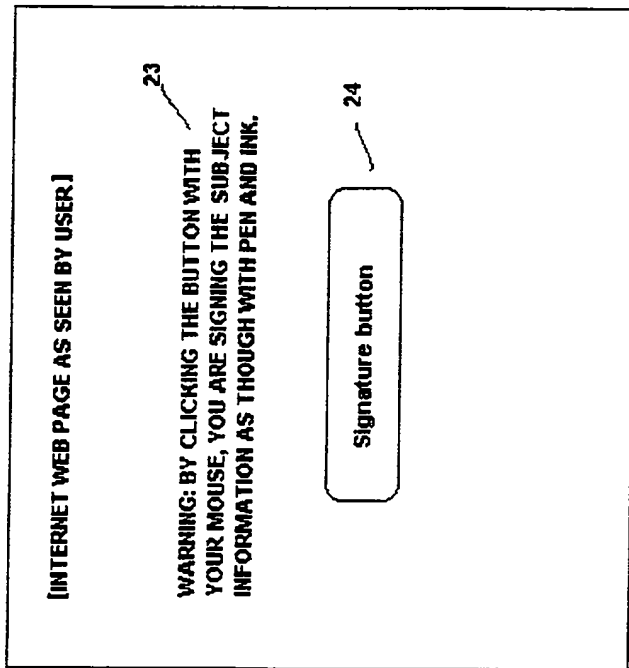


Figure 5

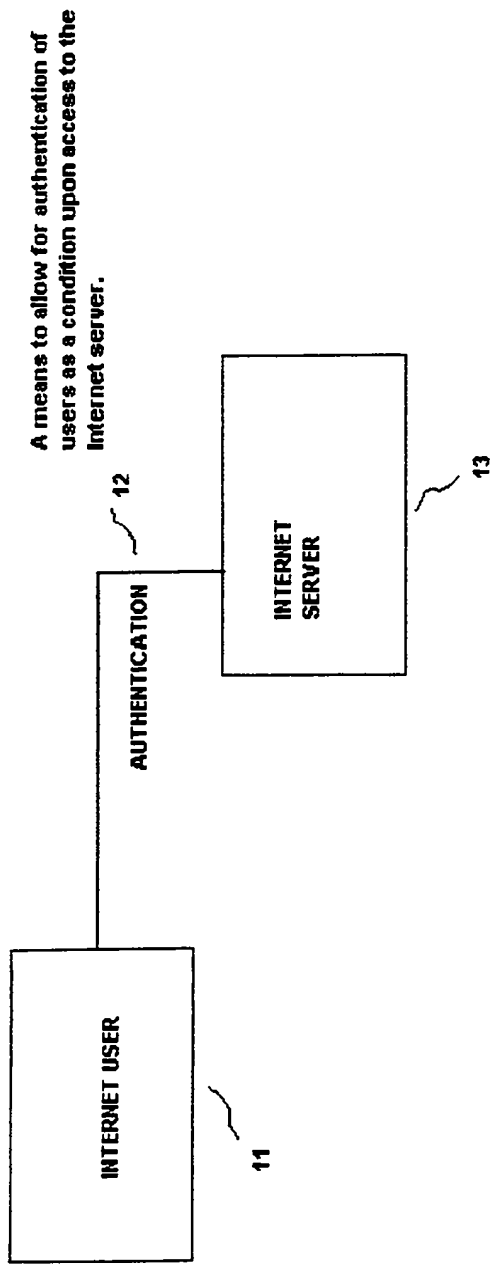


Figure 1

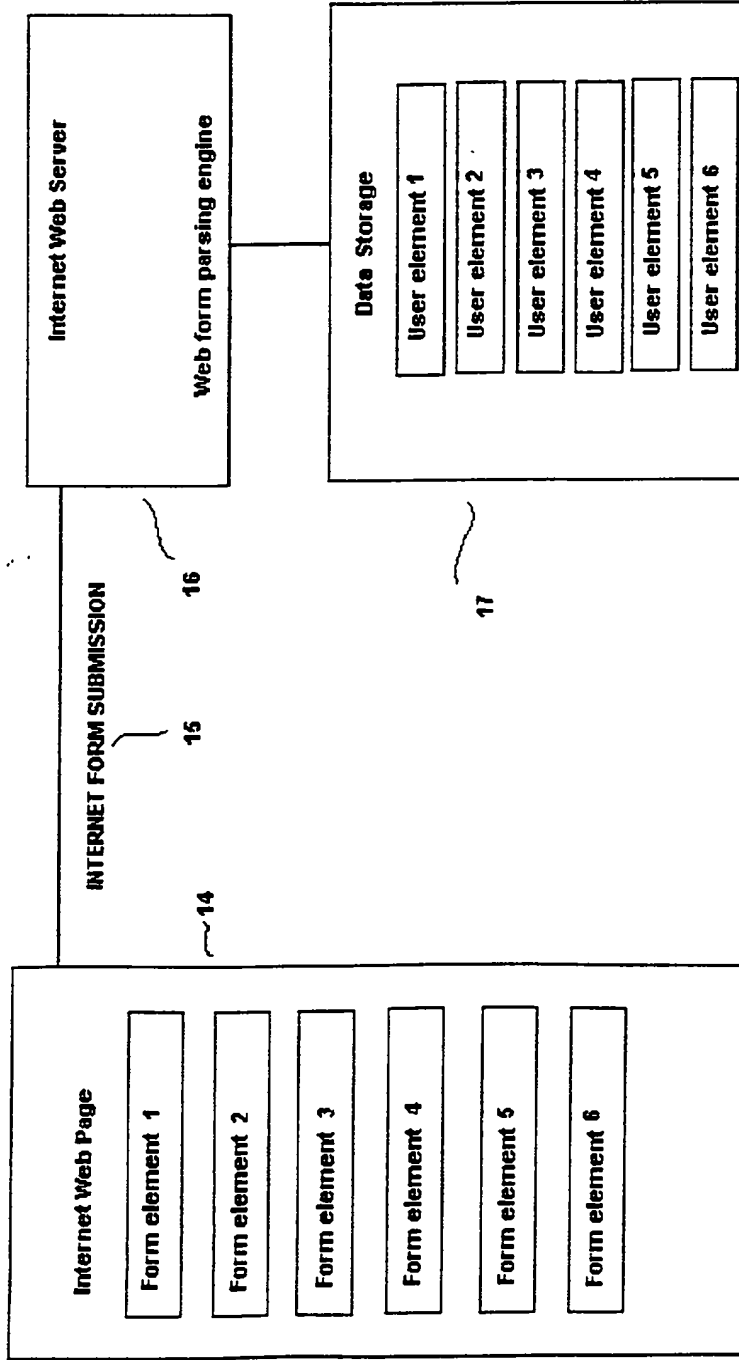


Figure 2

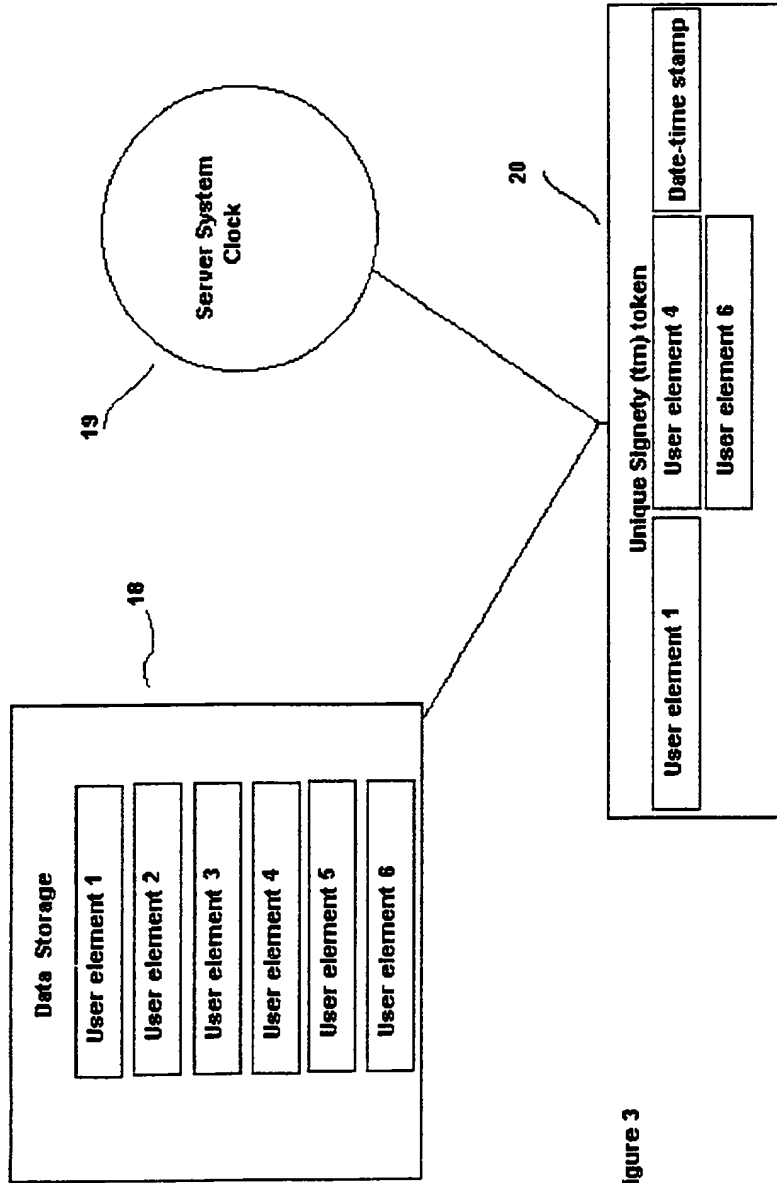


Figure 3

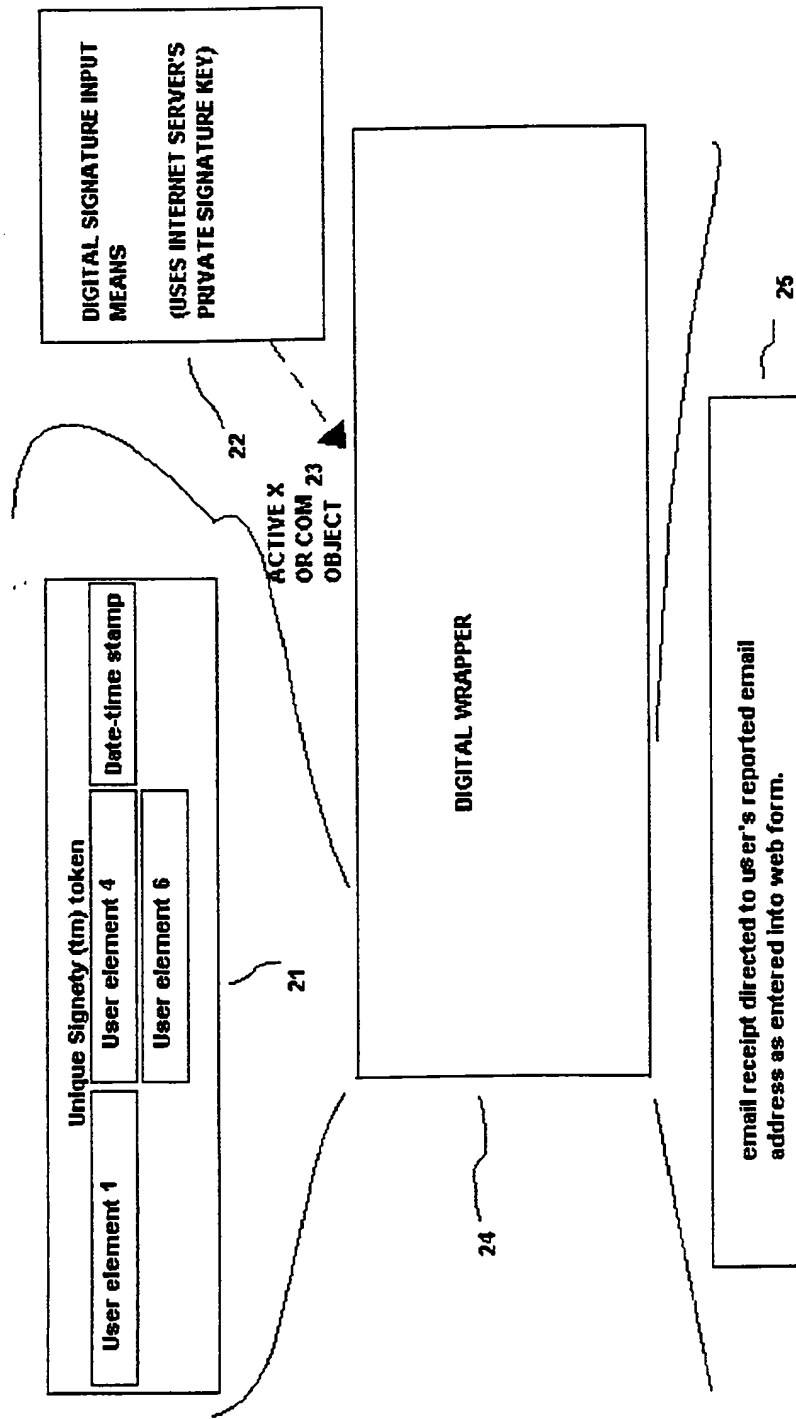


Figure 4

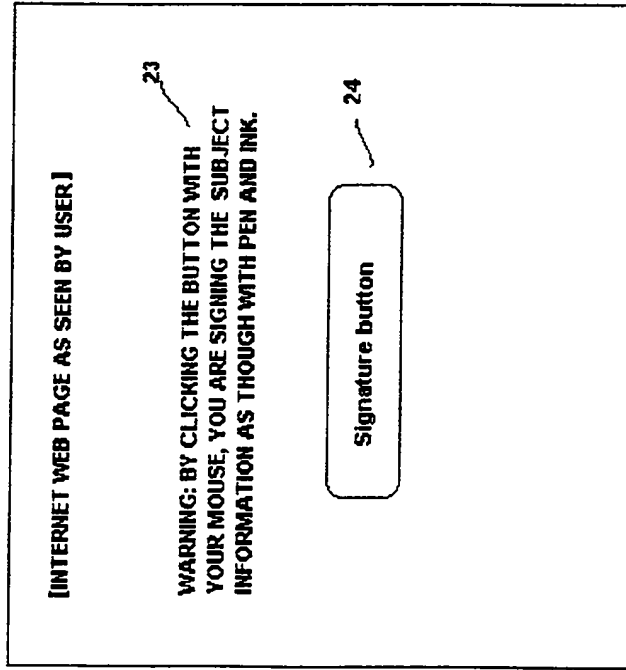


Figure 5

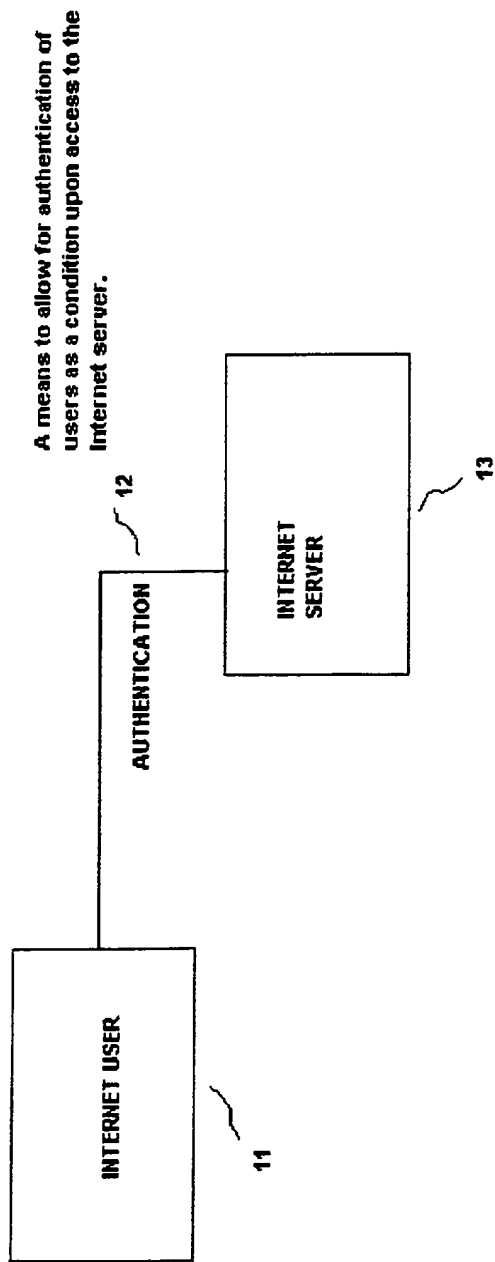


Figure 1

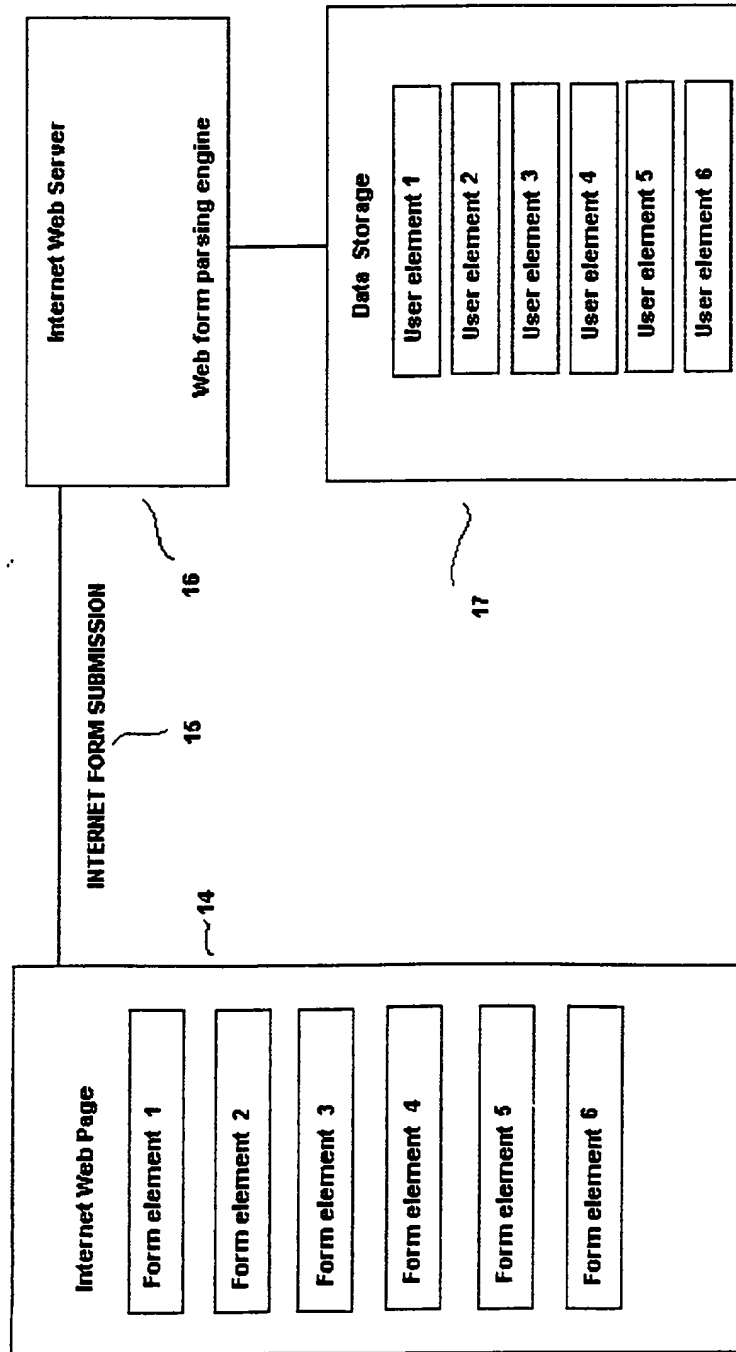


Figure 2

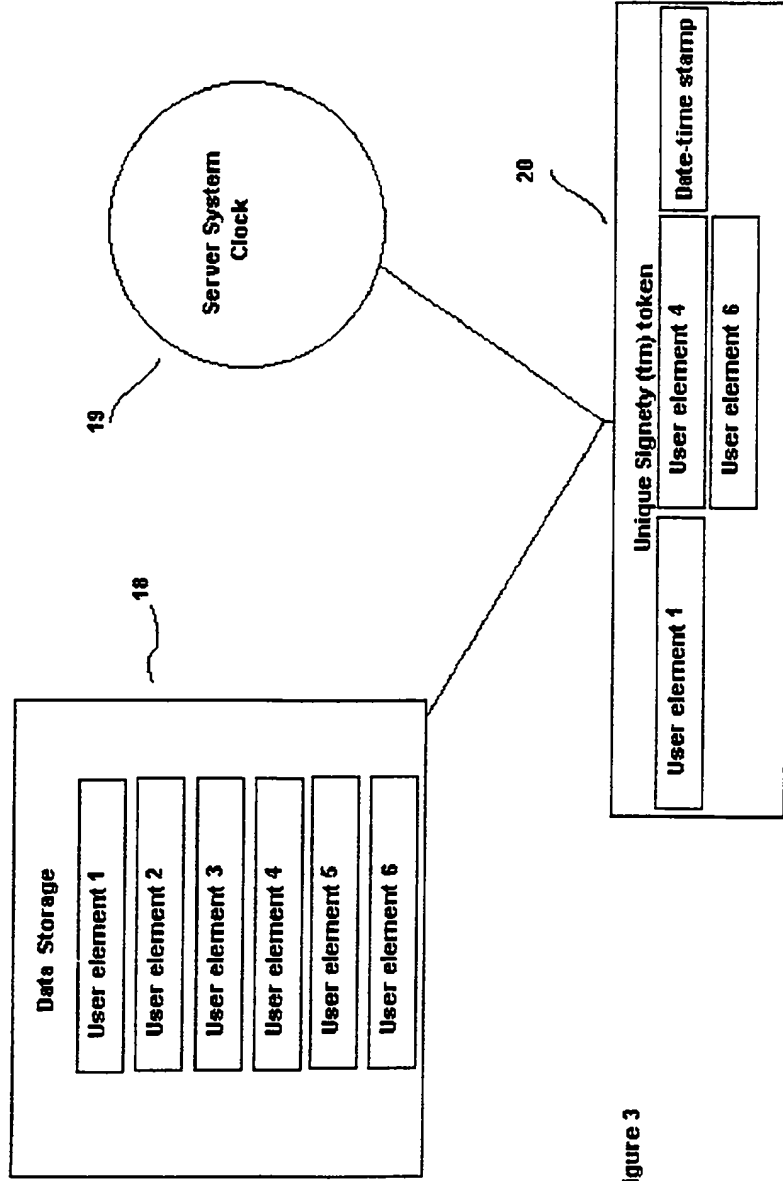


Figure 3

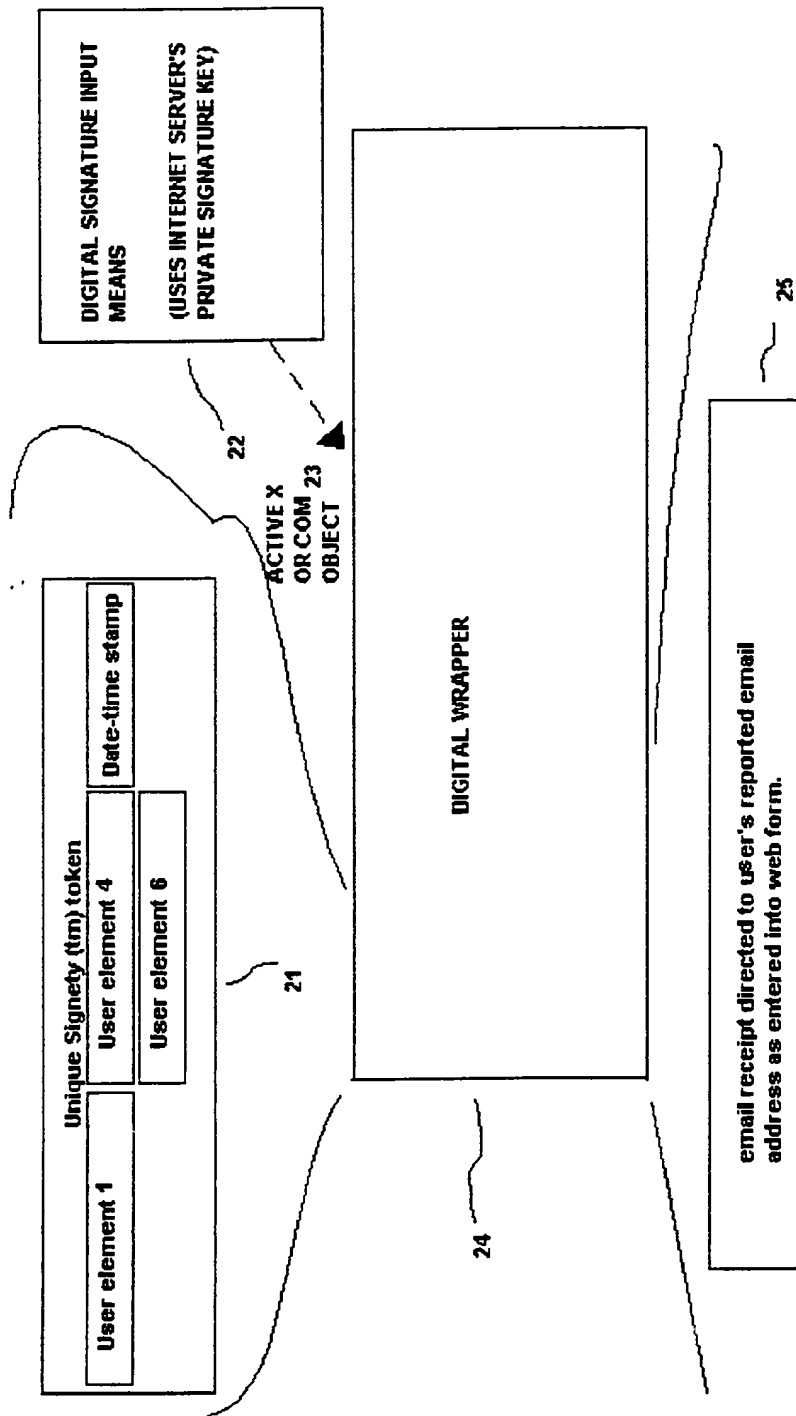


Figure 4

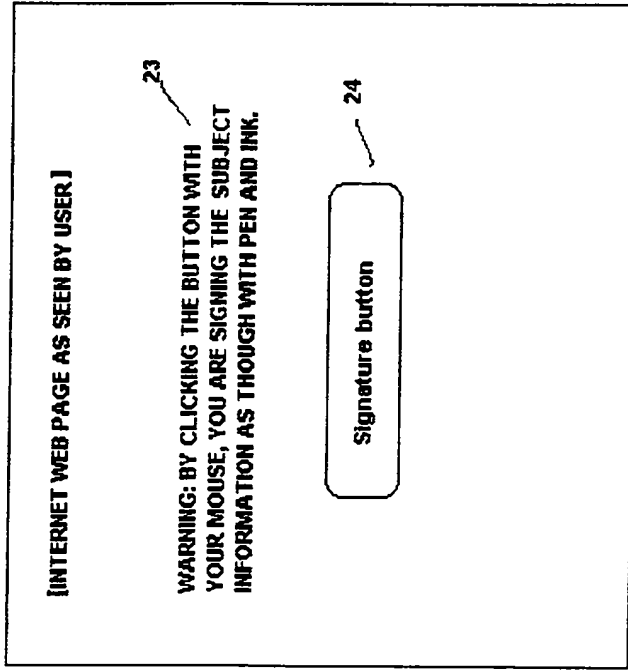


Figure 5